UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/506,815	04/11/2005	Arvind Ramaswamy	200601202-5	6801

22879 7590 09/20/2007

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
ALI, FARHAD	

ART UNIT	PAPER NUMBER
2146	

MAIL DATE	DELIVERY MODE
09/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/506,815	RAMASWAMY ET AL.	
	Examiner	Art Unit	
	Farhad Ali	2146	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 April 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *07 September 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *03/17/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

2. Claims 1-19 are rejected under 35 U.S.C. 102(e) as being anticipated by Fuh et al. (US 6,463,474 B1).

Fuh et al. teaches:

Claim 1

A data network management system for identifying unauthorized access to a data network service, provided at a service node in a data network, by a user node in said data network (Column 3 Lines 1-4, "a method of controlling access of a client to a network resource using a network device that is logically interposed between the client and the network resource"), said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network (Column 3 Lines 4-6, "the method comprising creating and storing client authorization information at the

network device," and Column 3 Lines 29-34, "creating and storing client authorization information comprises the steps of creating and storing in the network device a plurality of authentication caches, each authentication cache uniquely associated with one of a plurality of clients that communicate with the network device"), said system comprising:

a data communication means for periodically polling said agent at said service node and for retrieving a user access list from said agent (Column 3 Lines 39-44, "determining whether information in the request identifying the client matches information in a filtering mechanism of the network device and the authorization information stored in the network device");

a database for maintaining an authorized access list for said service node (See Figure 2, "Database"); and

a data processing means for comparing said user access list to said authorized user access list and for updating said authorized user access list, said authorized user access list being maintained in said database, an updated authorized user access list based on an updated user access list for said agent (Column 3 Lines 59-64, "when the source IP address fails to match the authorization information stored in the network device, determining if user identifying information received from the client matches a profile associated with the user that is stored in an authentication server that is coupled to the network device").

Claim 2

The data network management system as defined in claim 1, wherein said agent is a Simple Network Management Protocol agent (Applicant admits in desription of the Prior Art in Paragraph [0005] that "At present, the most pervasive tool is the Simple Network Management Protocol (SNMP)--a standard implemented in network nodes to publish information for the purposes of data network management).

Claim 3

The data network management system as defined in claim 1, wherein said data communication means is a Simple Network Management Protocol communication means (Applicant admits in desription of the Prior Art in Paragraph [0005] that "At present, the most pervasive tool is the Simple Network Management Protocol (SNMP)--a standard implemented in network nodes to publish information for the purposes of data network management).

Claim 4

The data network management system as defined in claim 1, further including means for installing said agent at said service node, said agent having means to communicate with said data communication means (Column 9 Lines 15-16, "A filtering mechanism 219 is part of the configuration of Authentication Proxy 400" which is a functional part of the network device).

Claim 5

A method for identifying unauthorized access to a data network service, provided at a service node in a data network, by a user node in said data network (Column 3 Lines 1-4, "a method of controlling access of a client to a network resource using a network device that is logically interposed between the client and the network resource"), said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network (Column 3 Lines 4-6, "the method comprising creating and storing client authorization information at the network device," and Column 3 Lines 29-34, "creating and storing client authorization information comprises the steps of creating and storing in the network device a plurality of authentication caches, each authentication cache uniquely associated with one of a plurality of clients that communicate with the network device"), said steps comprising:

a) periodically polling an agent and retrieving said user access list, for a given period of time, from said service node in said data network (Column 3 Lines 39-44, "determining whether information in the request identifying the client matches information in a filtering mechanism of the network device and the authorization information stored in the network device");

b) comparing said user access list to an authorized access list;

c) determining if said unauthorized access occurred based on said comparison step b) (Column 3 Lines 59-64, "when the source IP address fails to match the authorization information stored in the network device, determining if user

identifying information received from the client matches a profile associated with the user that is stored in an authentication server that is coupled to the network device");

d) if determined that said unauthorized access occurred in step c), initiating a notification process (Column 13 Lines 35-37, "If the authentication is not successful, as shown in block 736 and block 738, the process may notify the client with an appropriate message or page").

Claim 6

The method as defined in claim 5, further including a step of updating said authorized access list based on an updated user access list provided by said agent (Column 4 Lines 42-44, "updating the new authentication cache based on information received from the authentication server").

Claim 7

The method as defined in claim 5, further including a step of installing said agent at said user node, prior to periodically polling and retrieving said user access list in step a) (Column 9 Lines 15-16, "A filtering mechanism 219 is part of the configuration of Authentication Proxy 400" which is a functional part of the network device).

Claim 8

The method as defined in claim 5, further including a step of selecting said service node for identification based on a predetermined criteria, prior to retrieving said

user access list in step a) (Column 10 Lines 31-34, "Authentication Proxy 400 determines whether the source IP address in the header field of the packets corresponds to any entry in the filtering mechanism 219 configured in the Authentication Proxy 400. If the test of block 706 is affirmative, then control passes to block 708 in which the authentication caches are searched for the source IP address").

Claim 9

The method as defined in claim 5, wherein said notification process further including a step of notifying a Network Operations Console (Column 13 Lines 35-37, "If the authentication is not successful, as shown in block 736 and block 738, the process may notify the client with an appropriate message or page").

Claim 10

The method as defined in claim 5, wherein steps a) through c) are repeated, and wherein said user node is selected from one of a plurality of user nodes in said data network (Column 13 Lines 38-40, "Alternatively, Authentication Proxy 400 may permit Client 306 to re-try authentication a predetermined number of times").

Claim 11

The method as defined in claim 5, wherein steps a) through d) are repeated, and wherein said user node is selected from one of a plurality of user nodes in said data network (Column 13 Lines 38-40, "Alternatively, Authentication Proxy 400 may permit Client 306 to re-try authentication a predetermined number of times").

Claim 12

The method as defined in claim 5, wherein said agent is a Simple Network Management Protocol agent (Applicant admits in desription of the Prior Art in Paragraph [0005] that "At present, the most pervasive tool is the Simple Network Management Protocol (SNMP)--a standard implemented in network nodes to publish information for the purposes of data network management).

Claim 13

A computer-readable medium for identifying unauthorized access to a data network service, provided at a service node in a data network, by a user node in said data network (Column 3 Lines 1-4, "a method of controlling access of a client to a network resource using a network device that is logically interposed between the client and the network resource"), said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network (Column 3 Lines 4-6, "the method comprising creating and storing client authorization information at the network device," and Column 3 Lines 29-34, "creating and storing client authorization information comprises the steps of creating and storing in the network device a plurality of authentication caches, each authentication cache uniquely associated with one of a plurality of clients that communicate with the network device"), and said medium having stored thereon, computer-readable and computer-executable instructions which, when executed by a processor, cause said processor to perform steps comprising:

a) periodically polling an agent and retrieving said user access list, for a given period of time, from said service node in a data network (Column 3 Lines 39-44, "determining whether information in the request identifying the client matches information in a filtering mechanism of the network device and the authorization information stored in the network device");

b) comparing said user access list to an authorized access list;

c) determining if said unauthorized access occurred based on said comparison step b) (Column 3 Lines 59-64, "when the source IP address fails to match the authorization information stored in the network device, determining if user identifying information received from the client matches a profile associated with the user that is stored in an authentication server that is coupled to the network device");

d) if determined that said unauthorized access occurred in step c), initiating a notification process (Column 13 Lines 35-37, "If the authentication is not successful, as shown in block 736 and block 738, the process may notify the client with an appropriate message or page").

Claim 14

The computer-readable medium as defined in claim 13, further containing computer-readable and computer-executable instructions which perform a step of updating said authorized access list based on user access information (Column 4 Lines

42-44, "updating the new authentication cache based on information received from the authentication server").

Claim 15

The computer-readable medium as defined in claim 13, further containing computer-readable and computer-executable instructions which perform a step of installing said agent at said user node, prior to retrieving said user access list in step a) (Column 9 Lines 15-16, "A filtering mechanism 219 is part of the configuration of Authentication Proxy 400" which is a functional part of the network device).

Claim 16

The computer-readable medium as defined in claim 13, further containing computer-readable and computer-executable instructions wherein said steps a) through c) are repeated, and wherein said user node is selected from one of a plurality of user nodes in said data network (Column 13 Lines 38-40, "Alternatively, Authentication Proxy 400 may permit Client 306 to re-try authentication a predetermined number of times").

Claim 17

The computer-readable medium as defined in claim 13, wherein said agent is a Simple Network Management Protocol agent (Applicant admits in desription of the Prior Art in Paragraph [0005] that "At present, the most pervasive tool is the Simple Network Management Protocol (SNMP)--a standard implemented in network nodes to publish information for the purposes of data network management).

Claim 18

A computer for use in a data network for identifying unauthorized access to a data network service, provided at a service node in a data network, by a user node in said data network (Column 3 Lines 1-4, "a method of controlling access of a client to a network resource using a network device that is logically interposed between the client and the network resource"), said service node having an agent and having means for maintaining a user access list, said user access list having at least one data network address corresponding to at least one user node in said data network (Column 3 Lines 4-6, "the method comprising creating and storing client authorization information at the network device," and Column 3 Lines 29-34, "creating and storing client authorization information comprises the steps of creating and storing in the network device a plurality of authentication caches, each authentication cache uniquely associated with one of a plurality of clients that communicate with the network device"), said computer comprising:

a storage means (See Figure 1, "STORAGE DEVICE");

a central processing unit (See Figure 1, "PROCESSOR");

a data communication means for periodically polling said agent at said service node and retrieving a user access list from said agent (Column 3 Lines 39-44, "determining whether information in the request identifying the client matches information in a filtering mechanism of the network device and the authorization information stored in the network device");

said storage means having a database for maintaining an authorized access list for said service node (See Figure 2, "Database"); and

a data processing means for comparing said user access list to said authorized user access list and for updating said authorized user access list, said authorized user access list being maintained in said database, an updated authorized user access list based on an updated user access list for said agent (Column 3 Lines 59-64, "when the source IP address fails to match the authorization information stored in the network device, determining if user identifying information received from the client matches a profile associated with the user that is stored in an authentication server that is coupled to the network device").

Claim 19

The data network as defined in claim 1, wherein said authorized user access list is a common authorized user access list, and wherein said common authorization user access list includes a range of user nodes for comparing to said user access list to determine if said user access list is a subset of said common authorization user access list (See Figure 4 Number 432-436, "Authentification Cache").

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Farhad Ali whose telephone number is (571) 270-1920. The examiner can normally be reached on Monday thru Friday, 7:30am to 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeffrey C. Pwu can be reached on (571) 272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

F.A.

JEFFREY PWU
SUPERVISORY PATENT EXAMINER